



Transitive nonpropelinear perfect codes

I. Yu. Mogilnykh¹, F. I. Solov'eva¹

I. Yu. Mogilnykh and F. I. Solov'eva are with the Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia.

Abstract

A code is called transitive if its automorphism group (the isometry group) of the code acts transitively on its codewords. If there is a subgroup of the automorphism group acting regularly on the code, the code is called propelinear. Using Magma software package we establish that among 201 equivalence classes of transitive perfect codes of length 15 from [16] there is a unique nonpropelinear code. We solve the existence problem for transitive nonpropelinear perfect codes for any admissible length n , $n \geq 15$. Moreover we prove that there are at least 5 pairwise nonequivalent such codes for any admissible length n , $n \geq 255$.

© 2011 Published by Elsevier Ltd.

Keywords: perfect code, Mollard code, transitive action, regular action

2000 MSC: 94B25

1. Introduction

We consider codes in the Hamming space F_2^n of binary vectors of length n equipped with the Hamming metric. The Hamming distance $d(x, y)$ is the number of different coordinate positions of vectors x and y . The *code distance* of a code is the minimal value for the Hamming distance of its distinct codewords. The weight $wt(x)$ of a binary vector x of length n is defined as the Hamming distance between x and the all-zero vector 0^n . With a vector x we associate the collection of nonzero coordinates which we denote as $\text{supp}(x)$. A collection C of binary vectors of length n is called a *perfect* (1-perfect) code if any binary vector is at distance 1 from exactly one codeword of C .

Let x be a binary vector, π be a permutation of the coordinate positions of x . Consider the transformation (x, π) acting on a binary vector y by the following rule:

$$(x, \pi)(y) = x + \pi(y),$$

where $\pi(y) = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)})$. The composition of two automorphisms (x, π) , (y, π') is defined as follows

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi \circ \pi'),$$

where \circ is a composition of permutations π and π' .

Email addresses: ivmog@math.nsc.ru (I. Yu. Mogilnykh), sol@math.nsc.ru (F. I. Solov'eva)

¹The paper is accepted to publishing in Discrete Mathematics. The first author was supported by the Grants RFBR 12-01-00448 and 13-01-00463. The work of the second author was supported by the Grant RFBR 12-01-00631-a. Both authors are supported by the Grant NSh-1939.2014.1 of President of Russia for Leading Scientific Schools.

The automorphism group of the Hamming space F_2^n is defined as $\text{Aut}(F_2^n) = \{(x, \pi) : x \in C, \pi \in S_n, x + \pi(F_2^n) = F_2^n\}$ with the operation composition, here S_n denotes the group of symmetries of order n .

The *automorphism group* $\text{Aut}(C)$ of a code C is a collection of all transformations (x, π) fixing C setwise. In sequel for the sake of simplicity we require the all-zero vector to be always in the code. Then we have the following representation for $\text{Aut}(C)$: $\{(x, \pi), x \in C, \pi \in S_n, x + \pi(C) = C\}$.

A code C is called *transitive* if there is a subgroup H of $\text{Aut}(C)$ acting transitively on the codewords of C . If we additionally require that for a pair of distinct codewords x and y , there is a unique element h of H such that $h(x) = y$, then H acting on C is called a *regular group* [19] (sometimes called sharply-transitive) and the code C is called *propelinear* (for the original definition see [20]). In this case the order of H is equal to the size of C . If H is acting regularly on C , we can establish a one-to-one correspondence between the codewords of C and the elements of H settled by the rule $x \rightarrow h_x$, where h_x is the automorphism sending a certain prefixed codeword (in sequel the all-zero vector) to x . Each regular subgroup $H < \text{Aut}(C)$ naturally induces a group operation on the codewords of C in the following way: $x * y := h_x(y)$, such that the codewords of C form a group with respect to the operation $*$, isomorphic to H : $(C, *) \cong H$. The group is called a *propelinear structure* on C . The notion of propelinearity is important in algebraic and combinatorial coding theory because it provides a general view on linear and additive codes [5].

Two codes C and D are called *equivalent* if there is an automorphism ϕ of the Hamming space such that $\phi(C) = D$. Equivalence or permutational equivalence (i.e. when $\phi = (0^n, \pi)$) reduction is also often considered in problems of classification and existence for codes. Throughout in what follows we consider all codes to contain all-zero vectors. In this case for the class of transitive codes the notions of equivalence and permutational equivalence coincide.

For length 7, there is just one equivalence class of perfect codes, containing the Hamming code (a unique linear perfect code). A significant empirical boost of the study of perfect codes theory was made by Östergård and Pottonen who enumerated all equivalence classes of perfect codes of length 15 (see [16] for the database of the codes). In [17] it was established that 201 of 5983 such classes are transitive.

Papers of Avgustinovich [1], [2] provide a graphic point of view on the problem of equivalence of perfect codes by showing that two codes with isomorphic minimum distance graphs are equivalent. In light of this result, transitive and propelinear perfect codes have transitive and Cayley minimum distance graphs respectively [19]. This fact relates the topic of our work to a well known problem of the existence of transitive non-Cayley graphs.

Note the definitions imply that a propelinear code is necessarily transitive, however both topics were studied by several different authors and were developed somewhat independently.

In [22], [23] Solov'eva showed that the application of the Vasil'ev, Plotkin and Mollard constructions to transitive codes gives transitive codes. An analogous fact for propelinearity was shown for Vasil'ev codes earlier in [21] and later in [6] for the Plotkin and Mollard constructions. Studying 1-step switching class of the Hamming code, Malyugin [13] found several transitive perfect codes of length 15 (they were shown to be propelinear later in [6]).

The first nonadditive propelinear codes of different ranks were found in [6]. An asymptotically exponential of length class of transitive extended perfect codes constructed in [18] were shown to be propelinear in [7]. In [11] Potapov and Krotov utilized quadratic functions in the Vasil'ev construction to obtain propelinear perfect codes. Because these codes are only of small rank the question of the existence of a big (e.g. exponential of n) class of large rank propelinear perfect codes is still open.

The first transitive code that was shown not to have a propelinear representation was the well known Best code of length 10 and code distance 4 [6]. In the same work the question of the existence of transitive nonpropelinear perfect code was proposed.

The aim of this work is to separate the classes of transitive and propelinear perfect codes for any admissible length n . Using Magma software package, we found that only one of 201 transitive perfect codes of length 15 is nonpropelinear. The code is characterized in the class of transitive codes of length 15 by a unique property of having no triples from the kernel. The extension of this code by parity check gives a propelinear code. Since adding parity check preserves propelinearity of a code, we conclude that all extended perfect codes of length 16 are propelinear. In the paper we present the solution of the problem of the existence of transitive nonpropelinear perfect code for any admissible length n , $n \geq 15$. Moreover we show that there exist nonequivalent transitive nonpropelinear perfect code for any admissible length more than 127.

The current paper is organized as follows. Definitions and basic theoretical facts are given in the second section. The case $n = 15$ is considered in Section 3, where we give some information on the transitive nonpropelinear code and describe the way the search was carried out. A treatment of nonpropelinearity of the transitive nonpropelinear

code C of length 15 is in Section 4 as well as a sufficient condition for an extension of this property for the Mollard codes $M(C, D)$ for the appropriately chosen code D . The condition is essentially a restriction on the orbits of action of the symmetry groups of the Mollard codes. The condition holds if the Mollard code has certain metrical properties which we formulate by means of a numerical invariant $\mu_i(C)$ (the number of the triples from the kernel of the code incident to coordinate i). The main result of the paper is given in Section 5.

2. Preliminaries and notations

2.1. Mollard code

First give a representation for the Mollard construction [14]. Let C and D be two codes of lengths t and m . Consider the coordinate positions of the Mollard code $M(C, D)$ of length $tm + t + m$ to be pairs (i, j) from the set $\{0, \dots, t\} \times \{0, \dots, m\} \setminus (0, 0)$.

Let f be an arbitrary function from C to the set of binary vectors Z_2^m of length m and let $p_1(z)$ and $p_2(z)$ be the generalized parity check functions:

$$p_1(z) = \left(\sum_{j=0}^m z_{1,j}, \dots, \sum_{j=0}^m z_{t,j} \right),$$

$$p_2(z) = \left(\sum_{i=0}^t z_{i,1}, \dots, \sum_{i=0}^t z_{i,m} \right).$$

The code $M(C, D) = \{z \in Z_2^{tm+t+m} : p_1(z) \in C, p_2(z) \in f(p_1(z)) + D\}$ is called a Mollard code. In the case when C and D are perfect, the code $M(C, D)$ is perfect. Throughout the paper we consider the case when f satisfies $f(p_1(z)) = 0^m$ for any $p_1(z) \in C$.

A *Steiner triple system* is a set of n points together with a collection of blocks (subsets) of size 3 of points, such that any unordered pair of distinct points is exactly in one block. Further we put the triples of *STS* into round brackets to distinguish them with the supports of vectors. The set of codewords of weight 3 in a perfect code C , that contains the all-zero codeword defines a Steiner triple system, which we denote $STS(C)$.

By the Mollard construction it is easy to see that $STS(M(C, D))$ can be defined as

$$STS(M(C, D)) = \bigcup_{k,p \in \{0,3\}} T_{kp}, \text{ where}$$

$$T_{00} = \{(r, 0), (r, s), (0, s) : r \in \{1, \dots, t\}, s \in \{1, \dots, m\}\};$$

$$T_{33} = \{((r, s), (r', s'), (r'', s'')) : (r, r', r'') \in STS(C), (s, s', s'') \in STS(D)\};$$

$$T_{30} = \{((r, 0), (r', s), (r'', s)) : (r, r', r'') \in STS(C), s \in \{0, 1, \dots, m\}\};$$

$$T_{03} = \{((r, s), (r, s'), (0, s'')) : (s, s', s'') \in STS(D), r \in \{0, 1, \dots, t\}\}.$$

Denote by x^1 (y^2 respectively) the codeword in $M(C, D)$ such that $(x_{0,1}^1, \dots, x_{0,m}^1) = x \in C$ ($(y_{1,0}^2, \dots, y_{t,0}^2) = y \in D$ respectively) with zeros in all positions from $\{0, \dots, t\} \times \{1, \dots, m\}$ ($\{1, \dots, t\} \times \{0, \dots, m\}$ respectively). Note that $M(C, D)$ contains the codes C and D as the subcodes $M(C, 0^m) = \{x^1 : x \in C\}$ and $M(0^t, D) = \{y^2 : y \in D\}$ respectively.

Recall that the *dual* C^\perp of a code C is a collection of all binary vectors x such that $\sum_{i=1}^n x_i c_i = 0 \pmod{2}$ for any codeword c of C . Denote by $I(C)$ the following set:

$$I(C) = \{i : x_i = 0 \text{ for all } x \in C^\perp\}.$$

It is easy to see that

$$I(M(C, D)) = \{(r, s) : r \in I(C) \cup 0, s \in I(D) \cup 0\} \setminus (0, 0). \quad (1)$$

The *rank* of a code is defined to be the dimension of its linear span and the *kernel* of the code to be the subspace $\text{Ker}(C) = \{x \in C : x + C = C\}$. The rank and kernel are important code invariants. Due to its structure, the Mollard

code preserves many properties and characteristics of the initial codes, in particular, we have the iterative formulas for the size of kernel and rank:

$$\dim(\text{Ker}(M(C, D))) = \dim(\text{Ker}(C)) + \dim(\text{Ker}(D)) + tm, \quad (2)$$

$$\text{Rank}(M(C, D)) = \text{Rank}(C) + \text{Rank}(D) + tm. \quad (3)$$

The previous formula was used in [10] in solving the rank problem for propelinear perfect codes.

2.2. Automorphism group of a perfect code

The *symmetry group* $\text{Sym}(C)$ of a code C of length n (sometimes being called permutational automorphism group or full automorphism group [15]) is the collection of permutations on n elements with the operation composition, preserving the code setwise:

$$\text{Sym}(C) = \{\pi \in S_n : \pi(C) = C\}.$$

The *group of rotations*, see [3], [6], $\mathcal{R}(C)$, consists of all permutations with the operation composition, that could be embedded into the permutational part of an automorphism of C :

$$\mathcal{R}(C) = \{\pi : \text{there exists } x \in C \text{ such that } (x, \pi) \in \text{Aut}(C)\}.$$

Obviously, the symmetry group is a subgroup of the group of rotations. On the other hand, $\mathcal{R}(C)$ stabilizes the dual of the code and its kernel [19], [6], so we have

$$\text{Sym}(C) \leq \mathcal{R}(C) \leq \text{Sym}(\text{Ker}(C)), \quad (4)$$

$$\mathcal{R}(C) \leq \text{Sym}(C^\perp). \quad (5)$$

In section 5 we make use of the following known statement, which is a straightforward consequence of (5).

Lemma 1. *If $I(C)$ is the collection of zero coordinate positions for the dual of C , then $\mathcal{R}(C)$ stabilizes $I(C)$ setwise.*

Finally, the constant weight subcode of the code is stabilized by symmetries of the code, so in case of weight 3 we have

$$\text{Sym}(C) \leq \text{Aut}(\text{STS}(C)), \quad (6)$$

here and below by $\text{Aut}(\text{STS}(C))$ we mean the automorphism group of Steiner triple systems, i.e. the symmetry group of $\text{STS}(C)$ treated as a binary code.

Denote by $\mathcal{R}_x(C)$ the set of elements of $\mathcal{R}(C)$ associated with a codeword x of C :

$$\mathcal{R}_x(C) = \{\pi : (x, \pi) \in \text{Aut}(C)\}.$$

It is easy to see that the introduced sets are exactly cosets of $\mathcal{R}(C)$ by $\text{Sym}(C)$ (see [6]):

$$\mathcal{R}_x(C) = \pi \text{Sym}(C), \quad (7)$$

for any $\pi \in \mathcal{R}_x(C)$.

Now consider the Mollard code $M(C, D)$. For a permutation π on the coordinate positions of the code C , denote by $\mathcal{D}_1(\pi)$ a permutation on the coordinates of $M(C, D)$: $\mathcal{D}_1(\pi)(r, s) = (\pi(r), s)$ for $r \neq 0$ and $\mathcal{D}_1(\pi)(0, s) = (0, s)$ (see [23], [6]). For a permutation π on the coordinate positions of D , define $\mathcal{D}_2(\pi)(r, s) = (r, \pi(s))$ for $s \neq 0$ and $\mathcal{D}_2(\pi)(r, 0) = (r, 0)$.

If (x, π_x) and (y, π_y) are automorphisms of C and D respectively, then there is an automorphism $(z, \mathcal{D}_1(\pi_x)\mathcal{D}_2(\pi_y))$ of $M(C, D)$ for any z such that $p_1(z) = x$, $p_2(z) = y$, see [23]. In particular this fact shows that the Mollard construction preserves transitivity. So, we have the following facts:

Lemma 2. *Let C and D be perfect codes, z be a codeword of the Mollard code $M(C, D)$. Then*

1. $\mathcal{R}_z(M(C, D)) = \mathcal{D}_1(\mathcal{R}_{p_1(z)}(C))\mathcal{D}_2(\mathcal{R}_{p_2(z)}(D))\text{Sym}(M(C, D))$,
2. [23] $\mathcal{D}_1(\text{Sym}(C)) \leq \text{Sym}(M(C, D))$, $\mathcal{D}_2(\text{Sym}(D)) \leq \text{Sym}(M(C, D))$.

Lemma 3. [23] *If C and D are transitive codes, then $M(C, D)$ is transitive.*

3. Propelinear perfect codes of length 15

We give the original definition of a propelinear code. A code is called *propelinear* [20] if

- (i) each $x \in C$ could be assigned a coordinate permutation $\pi_x \in \mathcal{R}_x(C)$;
- (ii) the attached permutations satisfy:
if $(x, \pi_x)(y) = z$, then π_z is a composition of π_x and π_y , i. e. $\pi_z = \pi_x \circ \pi_y$, for any $y \in C$.

The property (i) is equivalent to transitivity of the group generated by the set of transformations $\{(x, \pi_x) : x \in C\}$. While the addition of the property (ii) amounts to the fact that the set of transformations $\{(x, \pi_x) : x \in C\}$ forms a group itself [19].

A *normalized propelinear code* [6] is defined by additionally requiring that the number of assigned permutations is minimal:

- (iii) $|\{\pi_x : x \in C\}| = |C|/|\text{Ker}(C)|$.

There are 201 perfect transitive codes of length 15, see [16]. See also [9] for more information on these codes, e.g. the sizes of ranks, kernels, etc. Using Magma [12], we studied the set of transitive perfect codes of length 15. For a given code, we checked if it is normalized propelinear [6], which is a relatively quick procedure. It turned out that there is just one transitive code (number 4918 in the database [16]), which is not normalized propelinear, while the other 200 codes admit a normalized propelinear structure (and therefore are propelinear). Moreover, a further search showed that there is no regular subgroup of the automorphism group of the code number 4918, so the code is nonpropelinear. This code of length 15 has a characteristic property of having the minimum distance of its kernel equaled 4, while remaining 200 transitive codes of length 15 have this parameter equal to 3.

Proposition 1. *There is a unique transitive nonpropelinear perfect code of length 15.*

The Steiner triple system of the transitive nonpropelinear code has rank 14 and therefore has a unique subsystem of order 7, see [8], on the coordinate positions $\{1, 2, 3, 4, 6, 7, 8\}$. Note that $\text{Aut}(\text{STS}(C))$ fixes the coordinates of a unique subsystem of order 7 setwise.

Table 1. Steiner triple system of the transitive nonpropelinear code of length 15

SubSTS				
(1, 3, 7)	(6, 11, 12)	(1, 5, 9)	(5, 7, 13)	(8, 10, 15)
(3, 6, 8)	(1, 11, 14)	(6, 10, 14)	(7, 9, 10)	(2, 14, 15)
(1, 4, 8)	(4, 10, 11)	(5, 8, 14)	(1, 12, 15)	(4, 5, 12)
(1, 2, 6)	(3, 10, 12)	(6, 9, 13)	(5, 6, 15)	(8, 12, 13)
(2, 3, 4)	(1, 10, 13)	(3, 13, 15)	(7, 12, 14)	(3, 9, 14)
(4, 6, 7)	(2, 9, 12)	(2, 5, 10)	(4, 13, 14)	(2, 11, 13)
(2, 7, 8)	(8, 9, 11)	(3, 5, 11)	(7, 11, 15)	(4, 9, 15)

The following permutations, together with the identity permutation form $\text{Aut}(\text{STS}(C))$, which coincides with $\text{Sym}(C)$:

$$(5, 15)(9, 12)(10, 14)(11, 13),$$

$$(5, 10)(9, 13)(11, 12)(14, 15),$$

$$(5, 14)(9, 11)(10, 15)(12, 13).$$

We define the transitive nonpropelinear perfect code of length 15 using its cosets of kernel, see Tables 2 and 3.

In Table 4 we give some parameters of the considered codes in this paper. The codes have special properties, which we will use later in Section 5. Let C be a code of length n , then for any $i \in \{1, \dots, n\}$ define $\mu_i(C)$ to be the

Table 2. Supports of the base of $\text{Ker}(C)$

$\{9, 11, 12, 13\}$	$\{4, 6, 7, 8, 11, 12, 14, 15\}$
$\{5, 12, 13, 14\}$	$\{2, 3, 6, 7, 11, 13, 14, 15\}$
$\{10, 12, 13, 15\}$	$\{1, 6, 7, 12, 13\}$

Table 3. Supports of the cosets of $\text{Ker}(C)$

$\{1, 12, 15\}$	$\{4, 6, 7\}$	$\{2, 4, 7, 10, 12\}$	$\{5, 6, 8, 9\}$
$\{4, 9, 15\}$	$\{4, 6, 14, 15\}$	$\{2, 11, 13\}$	$\{1, 4, 8\}$
$\{3, 9, 14\}$	$\{5, 7, 13\}$	$\{1, 2, 6\}$	$\{3, 5, 7, 12\}$
$\{4, 13, 14\}$	$\{1, 3, 7\}$	$\{2, 6, 8, 13, 15\}$	$\{2, 4, 9, 13\}$
$\{2, 8, 10, 11\}$	$\{8, 9, 11\}$	$\{3, 6, 8\}$	$\{6, 9, 13\}$
$\{5, 7, 8, 15\}$	$\{1, 5, 9\}$	$\{2, 5, 6, 13\}$	$\{6, 10, 14\}$
$\{2, 5, 10\}$	$\{3, 4, 5, 13\}$	$\{3, 13, 15\}$	$\{7, 11, 15\}$
$\{2, 7, 8\}$	$\{6, 8, 12, 15\}$	$\{3, 5, 8, 10\}$	

number of triples from $\text{Ker}(C)$ that contain i . From (4) and (6) we see that $\mu_i(C) \neq \mu_j(C)$ implies that the coordinates i and j are in different orbits of the group action of $\text{Sym}(C)$ on the coordinate positions $\{1, \dots, n\}$. In Table 4 and further $\mu(C)$ is the multiset collection of $\mu_i(C)$ denoted by $\mu_{k_1}^{i_1} \mu_{k_2}^{i_2} \dots \mu_{k_p}^{i_p}$, $p \leq n$ (here the integer μ_{k_l} appears i_l , $i_l \neq 0$ times, $1 \leq l \leq p$) for any coordinate i of C .

Table 4. Some transitive perfect codes of length 15

Code number in [16]	$\text{Rank}(C)$	$\text{Dim}(\text{Ker}(C))$	$ \text{Sym}(C) $	$\mu(C)$	$ \text{Aut}(\text{STS}(C)) $	$\text{Rank}(\text{STS}(C))$
51	13	7	8	$1^{13}3^15^1$	8	13
694	13	8	32	$1^83^55^2$	32	13
724	13	8	32	$1^{13}3^15^1$	96	13
771	13	8	96	$1^{12}3^3$	288	13
4918	14	6	4	0^{15}	4	14

4. Transitive nonpropelinear perfect codes

We say that a codeword x of C has *the incorrect inverse*, if any element of $\mathcal{R}_x(C)$ is of order more than 2 and stabilizes $\text{supp}(x)$.

Proposition 2. *A code C containing a codeword x with the incorrect inverse is not propelinear.*

Proof: Suppose H is a regular subgroup of the automorphism group of C . Let $h_x = (x, \pi_x) \in H$ be the automorphism attached to x , i.e. h_x maps 0 into x . Then $h_x^{-1} = (\pi_x^{-1}(x), \pi_x^{-1}) \in H$ maps the all-zero codeword to $\pi_x^{-1}(x)$. Because H is a regular group, there is a unique element of H sending 0 to x . However we have that $\pi_x^{-1}(x) = x$ and therefore the automorphisms h_x and h_x^{-1} must be equal, because they both map the all-zero codeword to x . So we get that π_x^2 is the identity permutation for some $\pi_x \in \mathcal{R}_x(C)$, which contradicts the fact that x is a codeword with the incorrect inverse. ■

Corollary 1. *If C is a code containing a codeword x with the incorrect inverse, then $\text{Sym}(C)$ is of even order and stabilizes $\text{supp}(x)$ setwise.*

Proof: From the proof of Proposition 2 we have that for any $\pi_x \in \mathcal{R}_x(C)$ the transformation $(\pi_x^{-1}(x), \pi_x^{-1}) = (x, \pi_x^{-1})$ is the automorphism of C . So, the set $\mathcal{R}_x(C)$ is closed under inversion. This fact combined with the fact that the square of any element of $\mathcal{R}_x(C)$ is not the identity, implies that $|\mathcal{R}_x(C)|$ is even. Moreover since $\mathcal{R}_x(C)$ is a coset of $\text{Sym}(C)$, the group generated by the elements of $\mathcal{R}_x(C)$ contains $\text{Sym}(C)$ and therefore $\text{Sym}(C)$ inherits the property of stabilizing $\text{supp}(x)$ setwise from $\mathcal{R}_x(C)$, because $\mathcal{R}_x(C)$ is closed under inversion. ■

We make use of the following empirical fact, established by Magma software package.

Proposition 3. *The code number 4918 in classification of [16] is transitive and contains a codeword x , $\text{supp}(x) = \{2, 3, 4\}$ with the incorrect inverse.*

Lemma 4. *Let C and D be perfect codes of lengths t and m respectively, σ be a permutation from $\text{Sym}(M(C, D))$ that stabilizes the subcode $M(0^t, D)$ setwise. Then there is an element π in $\text{Sym}(C)$ such that for any coordinate (r, s) , $r \in \{1, \dots, t\}$, $s \in \{0, \dots, m\}$ it holds $\sigma(r, s) = (\pi(r), s')$ for some $s' \in \{0, \dots, m\}$.*

Proof: Let \bar{s} be in $\{1, \dots, m\}$. Consider the triple $((r, 0), (r, \bar{s}), (0, \bar{s}))$ in $M(C, D)$ for some $r \in \{1, \dots, t\}$. Let $\sigma(0, \bar{s})$ be $(0, s''')$, then $\sigma(r, \bar{s}) = (r', s')$ and $\sigma(r, 0) = (r'', s'')$ for some s', s'' and nonzero $r', r'' \neq 0$. From the description of the triple set in the Mollard code we see that $r'' = r'$, i.e. $\sigma((r, 0), (r, \bar{s}), (0, \bar{s}))$ is in T_{03} or T_{00} . In other words, σ acts as a permutation $\pi \in S_t$ on the first coordinate of coordinates-pairs (r, s) : $\sigma(r, s) = (\pi(r), s')$, for nonzero r and any $s \in \{0, \dots, m\}$. The permutation π belongs to $\text{Sym}(C)$ since σ should act as a permutation from $\text{Sym}(C)$ on the first coordinate of the subcode $M(C, 0^m)$: for all $x \in C$ we have $p_1(\sigma(x^1)) = p_1(\pi(x)^1) = \pi(x) \in C$ iff $\pi \in \text{Sym}(C)$. ■

The following statement gives a sufficient condition for a Mollard code to preserve the incorrect inversion property of one of the codes in terms of the code symmetries.

Lemma 5. *Let C be a perfect code, x be a codeword of C with the incorrect inverse, D be a perfect code of length m such that*

$$\text{for any } \sigma \in \text{Sym}(M(C, D)) \text{ we have } \sigma(M(0^t, D)) = M(0^t, D) \quad (8)$$

and

$$\text{for any } \sigma \in \text{Sym}(M(C, D)) \text{ we have } \sigma(x^1) \in M(C, 0^m). \quad (9)$$

Then x^1 is a codeword with the incorrect inverse in $M(C, D)$.

Proof: By Lemma 2 we have

$$\begin{aligned} \mathcal{R}_{x^1}(M(C, D)) &= \mathcal{D}_1(\mathcal{R}_x(C))\mathcal{D}_2(\mathcal{R}_{0^m}(D))\text{Sym}(M(C, D)) = \\ &= \mathcal{D}_1(\mathcal{R}_x(C))\mathcal{D}_2(\text{Sym}(D))\text{Sym}(M(C, D)) = \mathcal{D}_1(\mathcal{R}_x(C))\text{Sym}(M(C, D)). \end{aligned}$$

By Lemma 4 a permutation $\sigma \in \text{Sym}(M(C, D))$ sends any element $(r, 0)$ of $\text{supp}(x^1) = \{(r, 0) : r \in \text{supp}(x)\}$ to $(\pi(r), s)$ for some $\pi \in \text{Sym}(C)$ and $s \in \{0, \dots, m\}$. By Corollary 1 the permutation π stabilizes the codeword $x \in C$ with the incorrect inverse, so $\pi(r) \in \text{supp}(x)$ and by the condition (9) we have that s is 0, i.e. x^1 is stabilized by $\text{Sym}(M(C, D))$. Now if $\pi' \in \mathcal{R}_x(C)$, then $\mathcal{D}_1(\pi')(x^1) = \pi'(x)^1 = x^1$ because x is a codeword with the incorrect inverse in C . So $\mathcal{D}_1(\mathcal{R}_x(C))\text{Sym}(M(C, D))$ stabilizes x^1 .

By Lemma 4, we see that the action of an element from $\mathcal{D}_1(\mathcal{R}_x(C))\text{Sym}(M(C, D))$ on the first coordinate of the coordinates-pairs of $M(C, D)$ is realized by an element from $\mathcal{R}_x(C)$, so for any $\sigma \in \mathcal{D}_1(\mathcal{R}_x(C))\text{Sym}(M(C, D))$ there is π such that

$$\sigma^2(r, s) = (\pi^2(r), s'), \text{ for all } r \in \{1, \dots, t\}, s \in \{0, \dots, m\}.$$

From the equality above we see that the order of any element from $\mathcal{R}_{x^1}(M(C, D))$ is not less than that of any element of $\mathcal{R}_x(C)$ and therefore is more than 2. Thus the codeword x^1 of $M(C, D)$ has the incorrect inverse. ■

5. Transitive nonpropelinear Mollard codes

In this section we use of the parameters $\mu_r(C)$ and $\mu(C)$ in constructing transitive nonpropelinear Mollard codes. We utilize the iterative structure of $\text{STS}(M(C, D))$ and obtain formulas for $\mu_{(r,s)}(M(C, D))$ for the Mollard code $M(C, D)$ from $\mu_r(C)$ and $\mu_s(D)$. Further we derive a metric version of Lemma 5 and construct 5 infinite series of perfect transitive nonpropelinear Mollard codes. Recall that $\text{STS}(M(C, D))$ could be presented as the union of the following sets:

$$\begin{aligned} T_{00} &= \{((r, 0), (r, s), (0, s)) : r \in \{1, \dots, t\}, s \in \{1, \dots, m\}\}; \\ T_{33} &= \{((r, s), (r', s'), (r'', s'')) : (r, r', r'') \in \text{STS}(C), (s, s', s'') \in \text{STS}(D)\}; \\ T_{30} &= \{((r, 0), (r', s), (r'', s)) : \{r, r', r''\} \in \text{STS}(C), s \in \{0, \dots, m\}\}; \\ T_{03} &= \{((r, s), (r, s'), (0, s'')) : \{s, s', s''\} \in \text{STS}(D), r \in \{0, \dots, t\}\}. \end{aligned}$$

Lemma 6. *Let $M(C, D)$ be a Mollard code obtained from perfect codes C and D of length t and m respectively. Then*

1. $\mu_{(r,0)}(M(C, D)) = \mu_r(C)(m + 1) + m$;
2. $\mu_{(0,s)}(M(C, D)) = \mu_s(D)(t + 1) + t$;
3. $\mu_{(r,s)}(M(C, D)) = 1 + 2(\mu_s(D) + \mu_r(C) + \mu_r(C)\mu_s(D))$.

Proof: First of all we note that a triple $\Delta \in \text{Ker}(M(C, D))$ iff $p_1(\Delta) \in \text{Ker}(C)$ and $p_2(\Delta) \in \text{Ker}(D)$.

1. By the criteria above, since $T_{00} \subset \text{Ker}(C)$, a coordinate position $(r, 0)$ is contained in m kernel triples $((r, 0), (r, s), (0, s))$, $s = 1, \dots, m$ from T_{00} . Also $(r, 0)$ is in $(m + 1)\mu_r(C)$ triples $((r, 0), (r', s'), (r'', s'))$ from $\text{Ker}(M(C, D)) \cap T_{03}$, where $(r, r', r'') \in \text{Ker}(C)$, $s' = 0, \dots, m$.

2. The proof is analogous to that of the first statement.

3. The coordinate (r, s) is in just one kernel triple from T_{00} which is $((r, 0), (r, s), (0, s))$.

Moreover, this coordinate is contained in $2\mu_r(C)$ and $2\mu_s(D)$ triples from $T_{30} \cap \text{Ker}(M(C, D))$ and $T_{03} \cap \text{Ker}(M(C, D))$ respectively that are equal to the sets $\{((r, s), (r', s), (r'', 0)) : (r, r', r'') \in \text{Ker}(C), s = 0, \dots, m\}$ and $\{((r, s), (r, s'), (0, s'')) : (s, s', s'') \in \text{Ker}(D), r = 0, \dots, t\}$ respectively.

Finally, there are $2\mu_r(C)\mu_s(D)$ triples

$$\{(r, s), (r', s'), (r'', s'') : (r, r', r'') \in \text{Ker}(C), (s, s', s'') \in \text{Ker}(D)\}$$

from $T_{33} \cap \text{Ker}(M(C, D))$ containing (r, s) .

Summing up the number of triples for the above cases, we get the desired value for $\mu_{(r,s)}(M(C, D))$. ■

Recall that $\mu(C)$ is defined above to be the multiset collection of $\mu_i(C)$ for any coordinate i of C . So $\mu(C)$ could be considered as a code invariant. From Lemma 6 we immediately obtain

Corollary 2. *Let $\mu(C) \neq \mu(C')$ for codes C and C' containing 0^n . Then the codes $M(C, D)$ and $M(C', D)$ are nonequivalent.*

Now we consider several conditions on the initial codes in order for the Mollard construction to preserve the incorrect inversion property.

Theorem 1. *Let C be a perfect code of length t with a codeword x with the incorrect inverse.*

1. *If we have*

$$\text{supp}(x) \subseteq I(C), \tag{10}$$

$$\mu_r(C) < (t - 1)/2 \text{ for any } r \in \{1, \dots, t\}, \tag{11}$$

then x^1 is a codeword with the incorrect inverse in $M(C, H)$.

2. *If we have*

$$\mu_r(C) = 0 \text{ for any } r \in \{1, \dots, t\}, \tag{12}$$

$$0 < \mu_s(D) < \frac{m-1}{2} \text{ for any } s \in \{1, \dots, m\}, m \leq t, \quad (13)$$

then x^1 is a codeword with the incorrect inverse in $M(C, D)$.

3. If (10), (12) hold for C and (13) holds for D , then x^1 is a codeword with the incorrect inverse in $M(M(C, D), H)$ for any Hamming code H .

Proof: We show that the conditions of Lemma 5 are satisfied.

Let us look at the values of μ for the coordinates of the considered Mollard codes.

1. By Lemma 6 we have the following relations for any $r \in \{1, \dots, t\}$ and $s \in \{1, \dots, m\}$:

$$\mu_{(r,0)}(M(C, H)) = \mu_r(C)(m+1) + m < (m+1)(t-1)/2 + m = \frac{tm+t+m-1}{2},$$

$$\mu_{(0,s)}(M(C, H)) = (m-1)(t+1)/2 + t = \frac{tm+t+m-1}{2},$$

$$\mu_{(r,s)}(M(C, H)) = 1 + 2\mu(C, r) + m - 1 + (m-1)\mu(C, s) = m + \mu(C, s)(m+1) = \mu_{(r,0)}(M(C, H)).$$

We see that the nonzero coordinates $\{(0, s) : s = 1, \dots, m\}$ of the subcode $M(0^t, H)$ are the only coordinates of $M(C, H)$ with the maximum possible value for μ . Therefore these coordinates are stabilized by $\text{Sym}(M(C, H))$ and we have the condition (8).

By (1) and (10) we obtain that $\text{supp}(x^1) = \{(r, 0) : r \in \text{supp}(x)\}$ is a subset $I((M(C, H))) = I(C) \times 0$ of zero coordinate positions for the dual of $M(C, H)$. By Lemma 1 we have that $\text{Sym}(M(C, H))$ stabilizes the block $I((M(C, H)))$ setwise, so the condition (9) holds.

2. We have the following relations for any $r \in \{1, \dots, t\}$ and $s \in \{1, \dots, m\}$:

$$\mu_{(r,0)}(M(C, D)) = \mu_r(C)(m+1) + m = m,$$

$$\mu_{(0,s)}(M(C, D)) = \mu_s(D)(t+1) + t > m,$$

$$\mu_{(r,s)}(M(C, D)) = 1 + 2(\mu_r(C) + \mu_s(D) + \mu_r(C)\mu_s(D)) = 1 + 2\mu_s(D) < m.$$

The above implies that the sets $\{(r, 0) : r = 1, \dots, t\}$, $\{(0, s) : s = 1, \dots, m\}$ and $\{(r, s) : s = 1, \dots, m, r = 1, \dots, t\}$ of coordinates of $M(C, D)$ are stabilized by $\text{Sym}(M(C, D))$, which implies that the conditions (8) and (9) hold.

3. We show that the hypothesis of the first statement of the theorem is true for the code $M(C, D)$ and a codeword x^1 . By the second statement of the theorem, the code $M(C, D)$ contains a codeword x^1 with the incorrect inverse. Moreover the block $\text{supp}(x^1)$ is a subset $I((M(C, D))) = (I(C) \cup 0) \times (I(D) \cup 0) \setminus (0, 0)$, i.e. the condition (10) is satisfied. Finally, from (12) and (13) we have that

$$\mu_{(r,0)}(M(C, D)) = m < \frac{tm+t+m-1}{2},$$

$$\mu_{(0,s)}(M(C, D)) = \mu_s(D)(t+1) + t < \frac{tm+t+m-1}{2},$$

$$\mu_{(r,s)}(M(C, D)) < m < \frac{tm+t+m-1}{2},$$

so the condition (11) is fulfilled for $M(C, D)$.

■

Theorem 2. 1. For $n = 15$ there is a unique transitive nonpropelinear code.

2. For any $n \geq 15$ there is at least one transitive nonpropelinear perfect code of length n .

3. For any $n \geq 255$ there are at least 5 pairwise inequivalent transitive nonpropelinear perfect codes of length n .

Proof: 1. See Proposition 1.

2. If C is a unique transitive nonpropelinear perfect code of length 15, then it fulfills the incorrect inversion property for x such that $\text{supp}(x) = \{2, 3, 4\}$, see Proposition 3. We show that the code $M(C, H)$ satisfies the condition of the previous theorem for any Hamming code H of length at least 1.

According to Table 1, $\text{supp}(x)$ is a triple of a unique subsystem of order 7 in $\text{STS}(C)$ (here STS is treated as a binary code). Since the coordinates of maximum order subsystems of STS are the complement of the supports of nonzero codewords in the dual code, see [8], we have that $\text{supp}(x) \subset I(\text{STS}(C))$. Since C and $\text{STS}(C)$ are both prefull rank codes (see Table 4) we have that $I(\text{STS}(C)) = I(C)$ and therefore (10) holds. Because there are no triples of C in $\text{Ker}(C)$, the condition (11) is also true.

3. The search shows that there are just 4 of 200 propelinear perfect codes of length 15 with the condition that any such code D fulfills (13): $0 < \mu_s(D) < 7$ for any $s \in \{1, \dots, 15\}$. These codes have numbers 51, 694, 724, 771 in [16] (see also Table 4). If D is any such code then the code $M(M(C, D), H)$ is nonpropelinear.

These four codes and the code $M(C, H')$ give five infinite series of nonpropelinear codes. From Table 4 we have that the triple (rank, kernel dimension, parameter μ) is a complete set of invariants determining inequivalence of the codes with numbers 51, 694, 724, 771. By (3) we see that the code $M(C, H')$ has smaller rank than any code of the type $M(M(C, D), H)$ of the same length. Moreover by (3), (2) and Corollary 2 the triple of invariants remains to be complete for the series of codes of the type $M(M(C, D), H)$.

■

In some sense, the characteristic $\mu_i(C)$ of a perfect code C could be seen as a measure of linearity of the coordinate i in the code. The transitive nonpropelinear perfect code of length 15 possesses the minimal linearity of coordinates, whereas the Hamming code gives the maximum.

The essence of Theorem 1 could be described informally: if we set C to be the transitive nonpropelinear code and choose D to be a propelinear code in a way that $\mu(D)$ is relatively "distant" to $\mu(C)$ in order to preserve its nonpropelinearity for $M(C, D)$, but not very "close" to $\mu(H)$ (where H is a Hamming code) so that $M(M(C, D), H)$ is nonpropelinear.

Acknowledgements This work was initiated while Ivan Mogilnykh was a visiting researcher at Combinatorics, Coding and Security Group of Department of Information and Communications Engineering in Autonomous University of Barcelona. He expresses his sense of appreciation to the Head of the group Professor J. Rifa for the hospital and warm stay. The authors are grateful to Josep Rifa and Quim Borges for stimulating discussions and critical remarks on the text.

References

- [1] Avgustinovich S.V.: On isometry of close-packed binary codes. *Siberian Adv. Math.* 5 (3) (1995) 1–4.
- [2] Avgustinovich S.V.: Perfect binary $(n, 3)$ codes: The structure of graphs of minimum distances. *Discrete Appl. Math.* 114 (2001) 9–11.
- [3] Avgustinovich S.V., Solov'eva F.I., Heden O.: On the structure of symmetry groups of Vasil'ev codes. *Probl. of Inform. Transm.* 5 (2005) 42–49.
- [4] Avgustinovich S.V., Solov'eva F.I., Heden O.: The classification of some perfect codes. *Des. Codes and Cryptogr.* 31 (3) (2004) 313–318.
- [5] Borges J., Rifa J.: A characterization of 1-perfect additive codes. *IEEE Trans. Inform. Theory* 54 (1999) 1688–1697.
- [6] Borges J., Mogilnykh I.Yu., Rifa J., Solov'eva F.I.: Structural properties of binary propelinear codes. *Advances in Math. of Commun.* 6 (3) (2012) 329–346.
- [7] Borges J., Mogilnykh I.Yu., Rifa J., Solov'eva F.I.: On the number of nonequivalent propelinear extended perfect codes. *The Electronic J. of Combinatorics* 20 (2) (2013) 37–50.
- [8] Doyen J., Hubaut X., Vandensavel M.: Ranks of incidence matrices of Steiner triple systems. *Mathematische Zeitschrift* 163 (3) (1978) 251–259.
- [9] Guskov G.K., Solov'eva F.I.: Properties of perfect transitive binary codes of length 15 and extended perfect transitive binary codes of length 16. *arxiv.org*, <http://arxiv.org/abs/1210.5940>.
- [10] Guskov G.K., Mogilnykh I.Yu., Solov'eva F.I.: Ranks of propelinear perfect binary codes. *Siberian Electronic Mathematical Reports* 10 (2013) 443–449.
- [11] Krotov D.S., Potapov V.N.: Propelinear 1-perfect codes from quadratic functions. *IEEE Trans. on Inform. Theory* 60 (2014) 2065–2068.
- [12] Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24 (1997) 235–265.
- [13] Malyugin S.A.: On equivalent classes of perfect binary codes of length 15". Preprint 138. Novosibirsk: Inst. of Mathematics of SB RAS. P. 34 (2004) (in Russian).
- [14] Mollard M.: A generalized parity function and its use in the construction of perfect codes. *SIAM J. Alg. Disc. Meth.* 7 (1) (1986) 113–115.
- [15] MacWilliams F.J., Sloane N.J.A.: *The Theory of Error-Correcting Codes*. North Holland, 1977.
- [16] Östergård P.R.J., Pottönen O.: The perfect binary one-error-correcting codes of length 15: Part I – Classification. *ArXiv*, <http://arxiv.org/src/0806.2513v3/anc/perfect15>.

- [17] Östergård P.R.J., Pottonen O., Phelps K. T.: The perfect binary one-error-correcting codes of length 15: Part II-Properties. *IEEE Trans. Inform. Theory*. 56 (2010) 2571–2582.
- [18] Potapov V.N.: A lower bound for the number of transitive perfect codes. *J. of Appl. and Industrial Math.* 1 (3) (2007) 373–379.
- [19] Phelps K. T., Rifa J.: On binary 1-perfect additive codes: some structural properties. *IEEE Trans. Inform. Theory*. 48 (2002) 2587–2592.
- [20] Rifa J., Basart J.M., Huguet L.: On completely regular propelinear codes. *Proc. 6th Int. Conference, AAECC-6. LNCS. 357* (1989) 341–355.
- [21] Rifa J., Pujol J., J. Borges J.: 1-Perfect Uniform and Distance Invariant Partitions. *Appl. Algebra in Engineering, Commun. and Computing*. 11 (2001) 297–311.
- [22] Solov'eva F.I.: On transitive codes. *Proc. Int. Workshop on Discrete Analysis and Operation Research. Novosibirsk, Russia. P. 99* (2004).
- [23] Solov'eva F.I.: On the construction of transitive codes. *Probl. of Inform. Transm.* 41 (3) (2005) 204–211.